The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:

12/1/2016

SUBJECT:

A Vulnerability in Mozilla Firefox Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has been identified in Mozilla Firefox, Firefox Extended Support Release (ESR), and Thunderbird, which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Mozilla Thunderbird is an email client. Successful exploitation may allow an attacker to execute remote code in the context of the user running the affected application or result in denial-of-service conditions. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

An exploit built on this vulnerability has been discovered in the wild targeting Tor browser users on Windows. The Tor browser operates through Firefox.

SYSTEM AFFECTED:

- Mozilla Firefox versions prior to 50.0.2
- Mozilla Firefox ESR prior to 45.5.1
- Thunderbird prior to 45.5.1

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A use-after-free vulnerability in Scalable Vector Graphics (SVG) Animation has been discovered, which allows an attacker to obtain target information, such as IP and MAC address, when the victim loads a webpage utilizing malicious JavaScript and SVG.

Successful exploitation may allow an attacker to execute remote code in the context of the user running the affected application or result in denial-of-service conditions. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2016-92/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9079

ARSTECHNICA:
http://arstechnica.com/security/2016/11/tor-releases-urgent-update-for-firefox-0day-thats-under-active-attack/

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/